

### **REMARKS**

The following remarks are prepared in response to the Office Action mailed October 4, 2004. Claims 1-56 are pending in this application, after entry of this amendment.

Claims 1-56 were rejected under 35 U.S.C. §102(b) as being anticipated by *Shrader* (U.S. Patent No. 5,864,666 hereinafter *Shrader*). Applicant respectfully traverses and requests reexamination.

#### **Rejection Under 35 U.S.C. §102(b)**

##### **Independent Claims 1, 17, 34 and 48**

The rejection of claims 1, 17, 34 and 48 should be withdrawn as *Shrader* fails to disclose all the recitations of these claims and therefore does not anticipate these claims.

Focusing on the specific recitations of claims 1, 17, 34 and 48 and the inadequacies of *Shrader*, claims 1, 34 and 48 recite, amongst other things: A secure network having a plurality of anti-bubbles where all of the network devices corresponding to at least one of the plurality of anti-bubbles have the same network security policy. Similarly, claim 17 recites, amongst other things, a secure network having a first and a second anti-bubble where each anti-bubble has a distinct network security policy.

The term “anti-bubble” is intended to refer to two or more devices that have no network access or connectivity with each other. (See paragraph 27 of the patent application.) Members of an anti-bubble have no network connectivity to any other members of the same anti-bubble. (See paragraph 49 of the patent application.) Moreover, members of any anti-bubble partition have no network connectivity to members of any other anti-bubble partition within the same anti-bubble. (See paragraph 49 of the patent application.) For example, as shown in figure 2, a device in anti-bubble partition 20a does not have network connectivity to any device in anti-bubble partition 20a or anti-bubble partition 20b. Furthermore, even

though all the devices within anti-bubble A have no network connectivity with respect to one another, they all have the same network security policy.

On page 2 of the Office Action, the Examiner incorrectly analogizes the term “anti-bubble” as recited in the claims with the term “operating systems” as disclosed in *Shrader*. In *Shrader*, when multiple computers are running on the same operating system, they are allowed to connect to one another if a firewall between the computers permits the connectivity. (See col. 4, lns. 11-14.) That is, the Internet firewall product allows administrators to create a physical firewall between an internal, secure network and the external, unsecure network of the internet. (See col. 4, lns. 11-14.) This is a conventional description of network connectivity and firewalls. By contrast, the claims recite a plurality of anti-bubbles where each anti-bubble includes two or more devices that have no network access or connectivity with each other. Hence, all the devices that belong to the same anti-bubble are prohibited from connecting to one another. *Shrader* fails to disclose multiple devices within a specific group that have no network access or connectivity with each other.

Also on page 2 of the Office Action, the Examiner directs Applicant to the concept of IP tunneling. *Shrader* discloses that a primary subject of the invention is IP tunneling. (See col. 4, lns. 47-48.) The administrator can define a tunnel between two internet firewalls that IP packets should flow through. (See col. 4, lns. 48-50.) The tunnel can impose authentication between the source and destination addresses as well as encrypt the IP packets flowing across the internet between the firewalls, depending on how the administrator defines the IP tunnel. (See col. 4, lns. 50-54.) IP tunneling sets up the flow of data between two devices. By contrast, anti-bubbles prohibit the flow of data between all devices within an anti-bubble while maintaining the same network security policy for all the devices within the same anti-bubble. This feature is not disclosed, taught or suggested by *Shrader*.

Therefore, for at least the two reasons discussed above — (1) a device in an anti-bubble does not have network connectivity to any other device in the same anti-bubble, and (2) all of the devices corresponding to at least one of the plurality of anti-bubbles have the same network security policy — *Shrader* does not disclose, teach or suggest all the features of claims 1, 17, 34 and 48. Accordingly, the rejection of claims 1, 17, 34 and 48 under 35 U.S.C. §102(b) should be withdrawn.

**Dependent Claims 2-16, 18-33, 35-47 and 49-56**

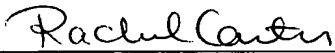
Claims 2-16 depend from independent claim 1, claims 18-33 depend from independent claim 17, claims 35-47 depend from independent claim 34, and claims 49-56 depend from independent claim 48. All of these dependent claims define the secure network with greater particularity and thus further distinguish over *Shrader*. For these reasons, and for the reasons set forth above with respect to independent claims 1, 17, 34 and 48, the rejection of these dependent claims should be withdrawn.

**Conclusion**

If there are any questions with regards to this prosecution, or if the Examiner believes that a telephone interview will help further the prosecution of the case, she is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 3, 2005.


By: Rachel Carter

  
\_\_\_\_\_  
Signature

Dated: January 3, 2005

Very truly yours,

**SNELL & WILMER L.L.P.**

  
\_\_\_\_\_  
Ketan S. Vakil  
Registration No. 43,215  
1920 Main Street, Suite 1200  
Irvine, California 92614-7230  
Telephone: (949) 253-4905